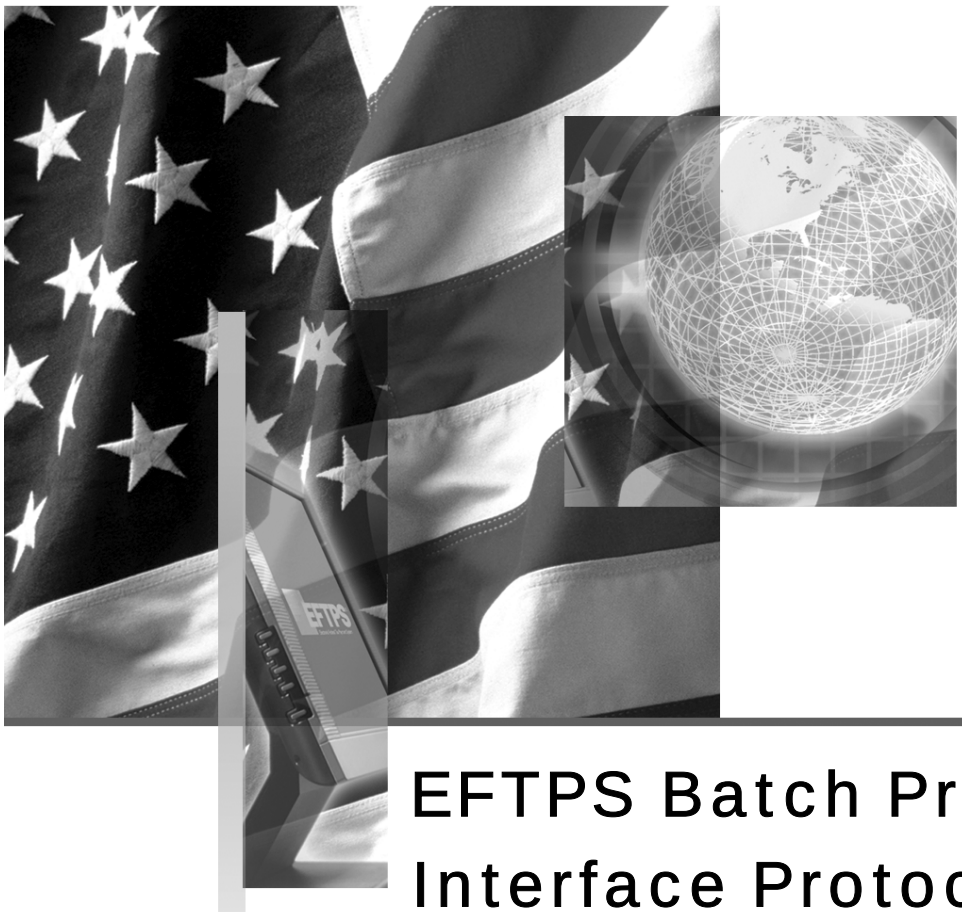

EFTPS Batch Provider Interface Protocol Specifications (IPS)

August 30, 2005

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

INTRODUCTION

The Electronic Federal Tax Payment System (EFTPS) Interface Protocol Specification (IPS) document defines a public XML Schema for performing a limited set of EFTPS taxpayer, batch provider and third party transmitter transactions. The schema defines a unique request and response XML element for each transaction. This document discusses the transactions and their associated schema elements.

BACKGROUND

Currently EFTPS batch providers interact with the EFTPS system through a combination of mailed-in paper forms and a Microsoft Windows PC client using a dial-in connection to EFTPS. Taxpayers who wish to use EFTPS interact through a VRS (voice response system) and the EFTPS-OnLine Website. The IPS augments the functionality of EFTPS by providing an XML-based interface for interaction with existing EFTPS taxpayer payment functionality using the pubic Internet. The IPS XML schema library provides a vocabulary for invoking EFTPS functionality; essentially a series of requests and associated responses.

INTENDED AUDIENCE

This document is meant to be accessible to the general technical business reader as well as software developers who will be developing applications that utilize the EFTPS IPS.

ASSUMPTIONS

It is assumed that the readers of this document have some familiarity with XML and XML Schema terminology as well as familiarity with general EFTPS business rules.

STANDARDS

SERVICES

The IPS is implemented as a "Web" service, but it does not conform to the WS-I basic profile (see http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html) because it does not support a SOAP envelope, nor does it define the service and operations through WSDL. It does however use schema that conforms to the W3C standards and recommendations and applicable IRS/FMS guidelines.

SCHEMA

The IPS XML Schema library uses a global namespace: http://www.eftps.gov/ips/1.0/. The namespace may change in future versions, where the last element of the path changes to 1.x or 2.x etc.. The schema is contained in one document that includes simple XML types, complex XML types, and the XML elements that represent request and response transactions.

TRANSPORT

Transactions take place over HTTPS.

IPS GUIDE

INTENDED USERS AND OPERATIONS

The IPS is designed to be used by both batch providers and third party transmitters/software developers. Taxpayers use the IPS through a third-party software intermediary.

Batch providers may use the IPS for the following EFTPS functions:

- Registration
    - Add New Batch Provider Registration
    - Add New Batch Provider Registration For Taxpayers Already Enrolled Or Batch Providers Already Registered In EFTPS (Express)
    - Submit Changes To Existing Batch Provider Registration
    - Registration Synchronization
- Enrollment
    - Add New Enrollments, Changes To Existing Enrollments, And Terminate Enrollments
    - Enrollment Synchronization
- Payment
    - Add New Payments And Cancel Scheduled Payments
    - Payment Synchronization
- Account Management
    - Change Master PIN
    - Change Master Password
    - Message Lookup
- Utility
    - Retrieve tax forms
    - Retrieve federal holidays
    - Retrieve international country codes

Taxpayers who are already enrolled with EFTPS and who have a PIN and an Internet Password may use the IPS for the following functions through a third party transmitter:

- Payment
    - Add New Payment Or Cancel Scheduled Payment
    - Payment Synchronization

IPS FUNCTIONALITY

The basic functionality of the EFTPS IPS application as manifested by the IPS/XML schema is shown below.

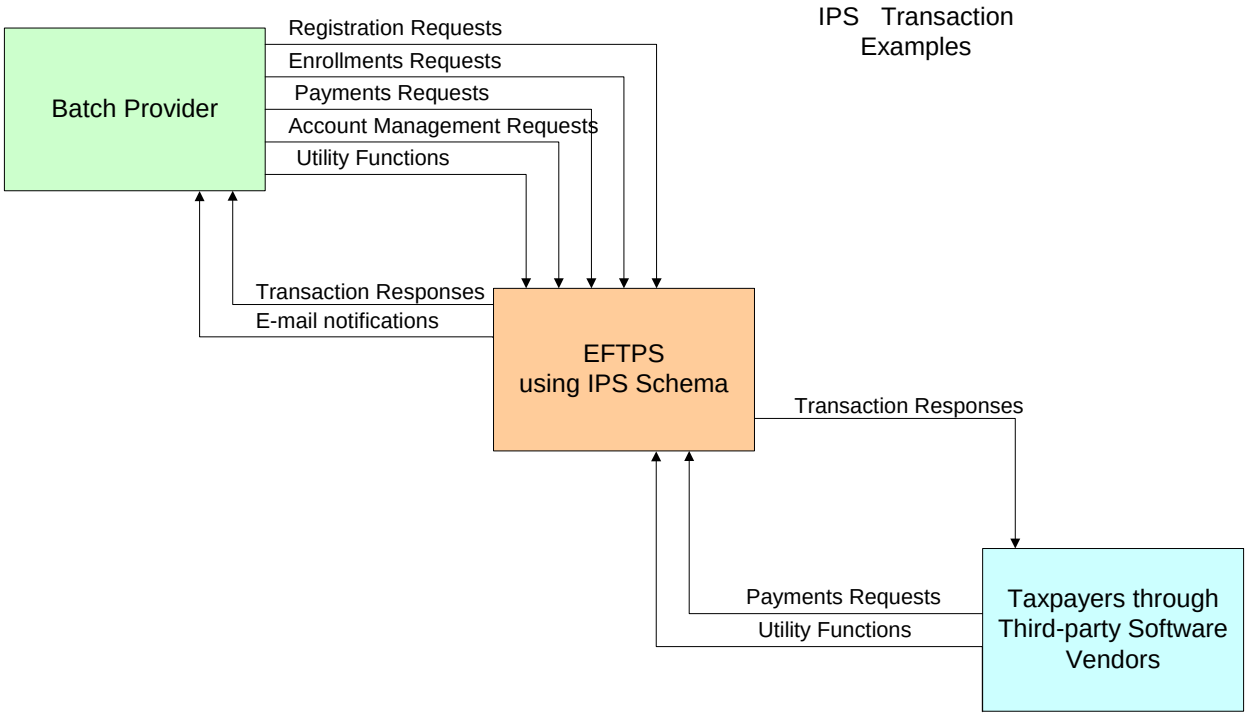

Figure 1 - Transaction schematic diagram

TRANSACTION SUMMARY

Transaction	Request XML Element, Response XML Element	Authentication	Timing
Registration			
Submit New Registration	BpRegistrationRequest, BpRegistrationResponse	None	Asynchronous
Change Registration	BpRegistrationRequest, BpRegistrationResponse	BpAuthentication	Asynchronous
Registration Synchronization	BpRegistrationSynchRequest, BpRegistrationSynchResponse	BpAuthentication	Synchronous
Payment			
Submit Payments And Payment Cancellations	BpPaymentRequest, BpPaymentResponse	BpAuthentication	Asynchronous
Get Payment History/ Payments Synchronization	BpPaymentSynchRequest, BpPaymentSynchResponse	BpAuthentication	Synchronous
Enrollment			
Submit Enrollments	BpEnrollmentRequest, BpEnrollmentResponse	BpAuthentication	Asynchronous
Enrollment Synchronization	BpEnrollmentSynchRequest, BpEnrollmentSynchResponse	BpAuthentication	Synchronous
Account Management			
Change Master Password	BpChangeMasterPasswordRequest, BpChangeMasterPasswordResponse	BpAuthentication	Synchronous
Change Master Pin	BpChangeMasterPINRequest, BpChangeMasterPINResponse	BpAuthentication	Synchronous
Message Request	BpMessageRequest, BpMessageResponse	BpAuthentication	Synchronous
Utilities			
Get Holidays	HolidayRequest, HolidayResponse	BpAuthentication	Synchronous
Get Tax Forms	TaxFormRequest, TaxFormResponse	BpAuthentication	Synchronous
Get Country Codes	CountryCodeRequest, CountryCodeResponse	BpAuthentication	Synchronous
Taxpayer Transactions			
Submit Payment, And Payment Cancellation	TpPaymentRequest, TpPaymentResponse	TpAuthentication	Synchronous
Get Payment History / Synchronization	TpPaymentSynchRequest, TpPaymentSynchResponse	TpAuthentication	Synchronous

Table 1: Transaction Summary with XML Schema Elements

TRANSACTION SUMMARY DETAILS

GENERAL INFORMATION

This section details each EFTPS IPS transaction. For each transaction, its use is described along with illustrative examples.

HEADERS

Request Header

All request messages are accompanied by an HTTP header named "RequestHeader" as part of the HTTP request. The header structure is the <RequestHeader> element as defined by the schema. This contains process environment information, software information, and authentication information.

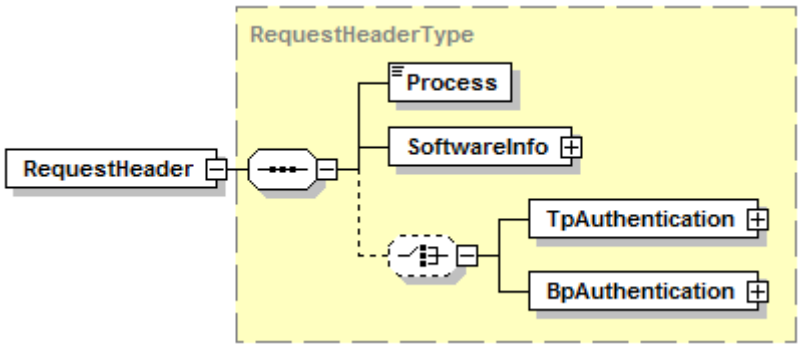

Figure 2 - Request Header

Requests submitted to the IPS application with incorrect environment information will be rejected. The allowed values for the <Process> element are: T (test) and P (production). Software information defines the originating software for all requests and responses. For transactions that originate with third-party software vendors, the SoftwareInfo element will be validated against the approved vendor list. The transaction requests that contain an unknown SoftwareInfo will be rejected.

Authentication requirements for each transaction type are shown in Table 1. Batch providers authenticate using the schema element <BpAuthentication>. The required elements for batch provider authentication are: batch provider Id, master PIN, and master Password. An example <RequestHeader> element with batch provider authentication is shown below:

```
<RequestHeader>
   <Process>T</Process>
   <SoftwareInfo>
      <SoftwareID>123456789</SoftwareID>
      <SoftwareName>Quicken</SoftwareName>
      <SoftwareVersion>1.0</SoftwareVersion>
   </SoftwareInfo>
   <BpAuthentication>
      <BPID>000000000</BPID>
      <MasterPIN>0000</MasterPIN>
      <MasterPassword>000000</MasterPassword>
   </BpAuthentication>
</RequestHeader>
```

Taxpayers authenticate using the schema element <TpAuthentication>. The required elements for taxpayer authentication are: EIN or SSN (TIN), PIN, and Internet Password. An example <RequestHeader> element with the taxpayer authentication nodeset is shown below:

```
<RequestHeader>
   <ProcessType>T</ProcessType>
   <SoftwareInfo>
      <SoftwareID>123456789</SoftwareIDVendor>
      <SoftwareName>QuickBooks</SoftwareName>
      <SoftwareVersion>1.0</SoftwareVersion>
   </SoftwareInfo>
   <TpAuthentication>
      <TIN>000000000</TIN>
      <PIN>0000</PIN>
      <InternetPassword>000000</InternetPassword>
   </TpAuthentication>
</RequestHeader>
```

Response Header

Similarly, the HTTP response contains a "Response`Header`" with the structure of the <ResponseHeader> element as defined by the schema. The important element in this header is the <Status>, which indicates if the request was successfully transmitted to the service. Any technical or security error conditions will be caught prior to processing requests, and these errors will be returned in the header. The idea is similar to the SOAP fault in the Web services world – non-business errors are handled here. As such, unless the <Status> is OK, there will not be a message body returned. This header also contains process environment information and software version information.

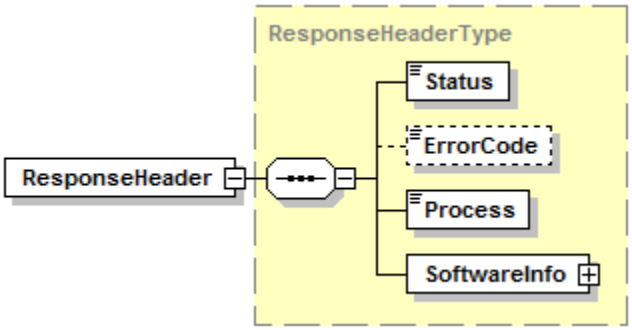

Figure 3 - Response Header

An example <ResponseHeader> element is shown below:

```
<ResponseHeader>
   <Status>OK</Status>
   <Process>T<Process>
   <SoftwareInfo>
      <SoftwareID>123456789</SoftwareIDVendor>
      <SoftwareName>Quicken</SoftwareName>
      <SoftwareVersion>1.0</SoftwareVersion>
   </SoftwareInfo>
</ResponseHeader>
```

Note that any header information used in the HTTP transport is lost downstream when a protocol swap occurs, because there is no message envelope in the body.

CONTROL RECORD

The EFTPS IPS application works through a combination of both synchronous and asynchronous transactions. Synchronous transactions are processed in real time by the IPS provider. For asynchronous transactions, the first step receives the initial batch provider request and immediately sends back a response. For requests that pass authentication and validation, a OK response will be returned. The second step requires the batch provider to transmit a synchronize request at a later time to determine if the requested processing has been completed.

All batch submissions (enrollments and payments) contain a control record which is comprised of a date, and a sequence number. Control records must be unique for all enrollment requests for a batch provider. Control records must be unique for all payment requests for a particular batch provider. Duplicate control records found in requests will cause the request to be rejected.

IPS RESPONSE BODY

The detailed transaction responses to a request are returned in the XML type <ResponseType>. All responses have two elements:

- Status
- ErrorCode

The <Status> element contains a single status tag to store a response status code that indicates the result of the transaction processing. The following table lists each possible status code value.

Code	Description	User Action
FMT	The XML request failed schema validation.	Correct and resend.
AUTH	The XML request was denied due to authentication constraints.	Correct and resend.
CPR	The account used to authenticate the request must change its password before proceeding.	Change password and resend.
PEND	The IPS provider received the request and results are pending. (This status does not apply to all requests.)	None.
OK	The IPS provider successfully processed the request and any transaction appropriate results are contained in the response.	None.
PART	Some of the records in the request did not pass business rule validation, but those that did were successfully processed by the IPS application. The request was completely processed.	Correct the records that failed and resend only those records.
ERR	The IPS provider was unable to process the request and should be contacted if the problem persists.	Retry later.

Table 2: Response Status Types

The <ErrorCode> element contains information on errors that occurred during processing. For example, if the request failed schema validation the <Status> element will be set to **FMT** and the <ErrorCode> element will contain information on the location of the validation errors.

For those transactions that contain multiple actions (e.g. submit enrollments or submit payments), in addition to the <ResponseType> element (which communicates the overall transaction result), a detailed response type (e.g. <PaymentDetailResponseType>) contains information on the status of each of the individual records in the request. The possible values for the <Status> element of these responses are shown in Table 3. Response detail elements also include an <ErrorCode> element to further identify the error that has occurred on a particular record of a transaction.

Code	Description	User Action
VAL	The XML request was invalid due to a failed field edit or business validation.	Correct and resend.
PEND	The IPS provider received the request and results are pending. (This status does not apply to all requests.)	None.
OK	The IPS provider successfully processed the request and any transaction appropriate results are contained in the response.	None.
PART	Some of the records in the request did not pass business rule validation, but those that did were successfully processed by the IPS application. The request was completely processed.	Correct the records that failed and resend only those records.

Table 3: Detail Status Types

Each request received by the IPS has an associated response detailed in the Transaction Summary section that follows. Responses contain both request level and detail level information.

For request level errors, a status and possibly an error will be returned.

BATCH PROVIDER REGISTRATION TRANSACTIONS

NEW BATCH PROVIDER REGISTRATION

All batch providers that plan to use the EFTPS IPS must register as a batch provider. Third party transmitters must send in a setup form to EFTPS. There are two types of new registrations, non-express and express.

Non-express Batch Provider Registration

- Used by batch providers that have not previously participated in EFTPS Batch Filer or EFTPS-OnLine and for whom IRS entity validation is required.

Express Batch Provider Registration

- Used by batch providers that have are currently registered as EFTPS Batch Filers or are an active taxpayer using the EFTPS-OnLine web site.
- This method allows the batch provider to pick their own master PIN to use as part of their authentication. The responses are the same as displayed for non-express registrations.

The XML schema element for the New Registration request is <BpRegistrationRequest>. Responses for New Registration requests are instances of the XML schema element <BpRegistrationResponse>. The schema is designed to trap the majority of data errors via the schema validation process. If a new registration passes all validation checks, the response will contain their batch provider registration number. EFTPS will then send the batch provider multiple packets via US mail that will include their batch provider registration number, their Master PIN (self selected for express registration) and information on how to complete their registration and obtain their Master Password.

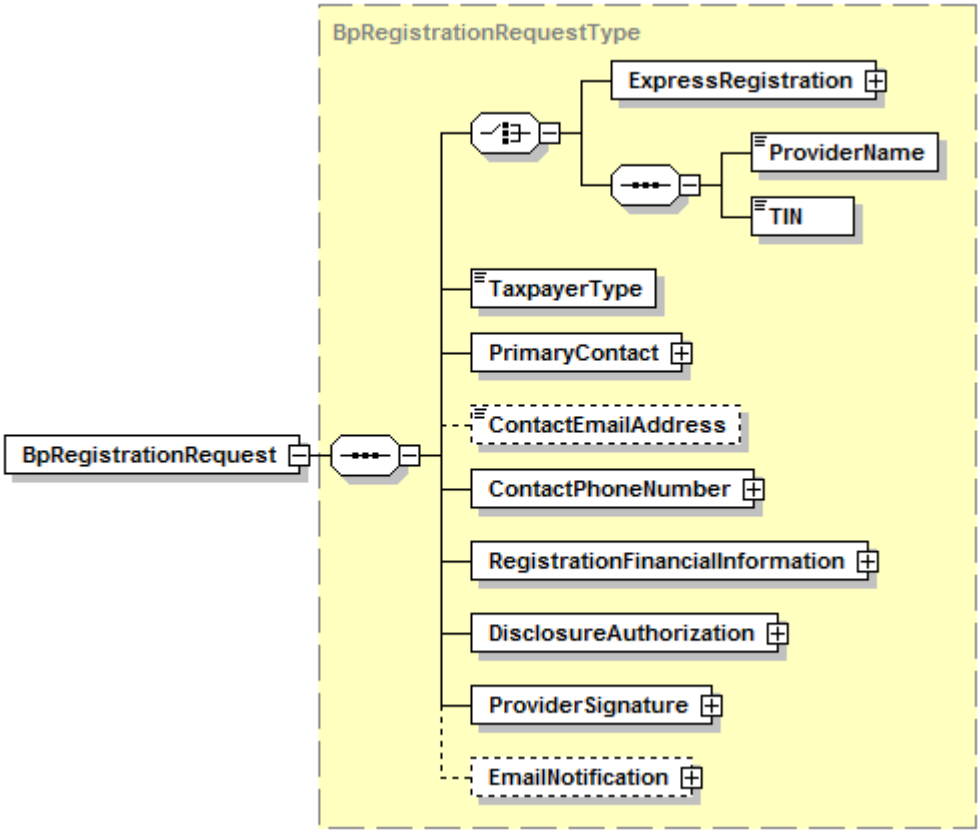

Figure 4 - Registration Request

CHANGE BATCH PROVIDER REGISTRATION (EDIT, EDIT FI, CANCEL EDIT FI)

The change batch provider registration transaction allows batch providers to make changes to existing registrations. The changes include changing financial and non-financial data. The XML schema element for the Change Registration request is <BpChangeRegistrationRequest>. Responses for the request are instances of the XML schema element <BpChangeRegistrationResponse>. A previously registered batch provider will need to obtain an master password from the EFTPS VRS for full authentication credentials. Batch provider authentication credentials must be sent as part of this request.

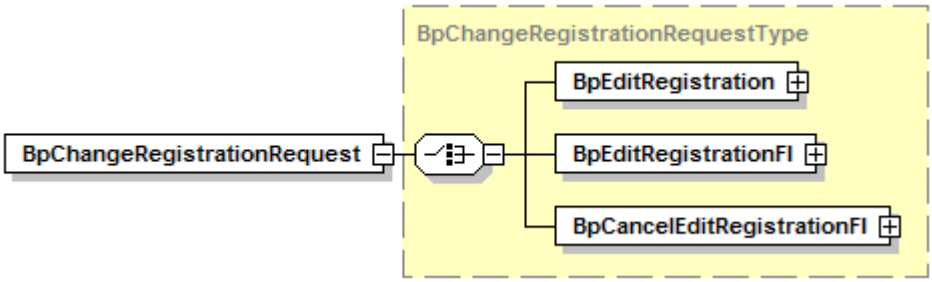

Figure 6 - Change Registration Request

Edit Batch Provider Registration (Non-Financial Information)

The edit batch provider registration should be used to update non-financial batch provider data within EFTPS. These changes, when EFTPS processing is complete, will be reflected back to clients via the registration synchronization request. Financial and IRS entity validated information cannot be changed with this request.

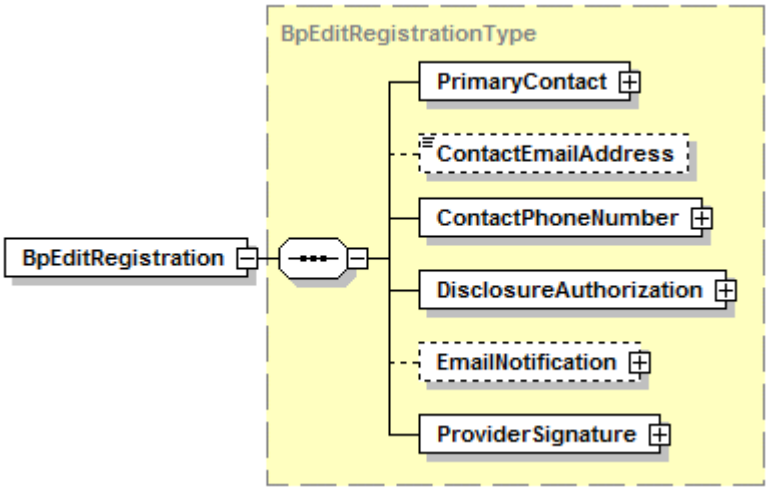

Figure 7 - Edit Registration

Edit Batch Provider Registration FI (Financial Information)

The edit batch provider registration FI request allows a batch provider to change their bank account information at a specified future date.

Only one edit registration FI request may be outstanding at a time for a batch provider. This means that if an edit registration FI request is received for a batch provider while there is another batch provider edit registration FI request pending, the pending request must first be cancelled (see Cancel Edit Registration FI). Edit registration FI requests that choose to prenote must have an effective date at least six business days in the future. Prenote failure notification will occur through the US mail.

Warehoused payments may be effected by this request. If there are warehoused payments with settlement dates past the effective date for a batch provider bank account change and the payments were made using the batch provider's bank account, those payments must be cancelled before the FI change will be allowed. Previously warehoused payments that were made using the taxpayer's bank account will not be effected by this request.

The possible responses for edit registration FI include OK, FMT, CPR, VAL, and ERR. The OK response indicates that the IPS application has successfully received and processed the request. If any of the other response statuses are found, the originating request will have to be corrected and resent.

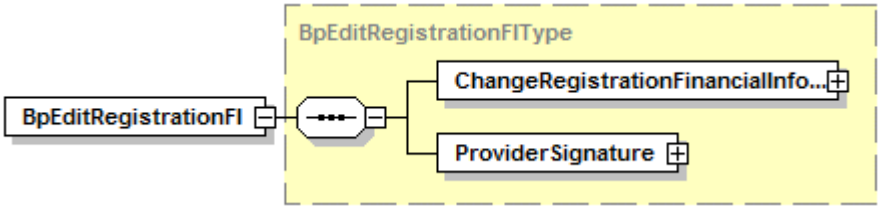

Figure 8 - Edit Registration FI

Cancel Edit Registration FI (Financial Information)

This function is used to cancel previous registration edit FI requests. A registration edit FI request may be cancelled up to one day before the effective date of the original request. If the request is eligible for cancellation, the bank account information that the batch provider was using prior to the edit FI request that is being cancelled will be reinstated. If the request is not eligible for cancellation, notification will be sent in the response.

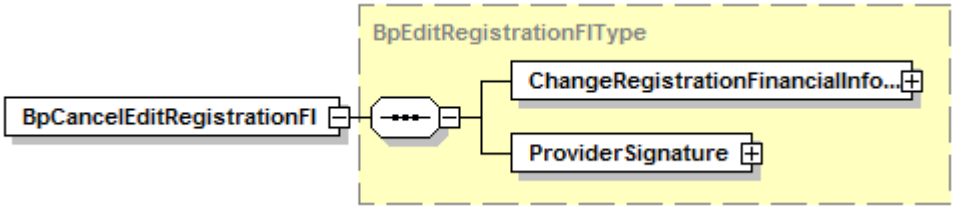

Figure 9 - Cancel Edit Registration FI

SYNCHRONIZE REGISTRATION

Registration synchronization is used by a batch provider to retrieve their registration information from the EFTPS IPS application. The XML schema element for the Synchronize Registration request is <BpRegistrationSynchRequest>. Responses are instances of the XML schema element <BpRegistrationSynchResponse>.

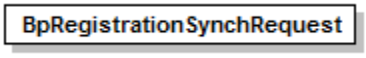

Figure 10 - Registration Sync Request

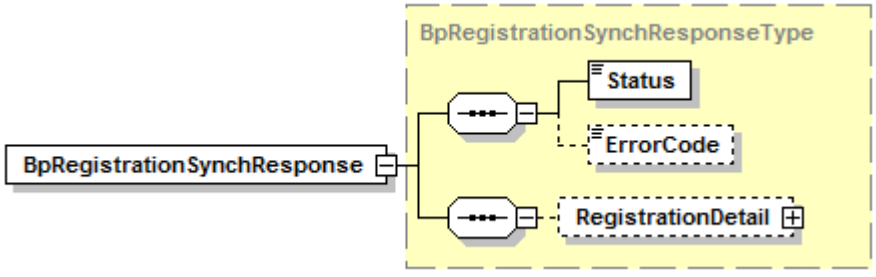

Figure 11 - Registration Sync Response

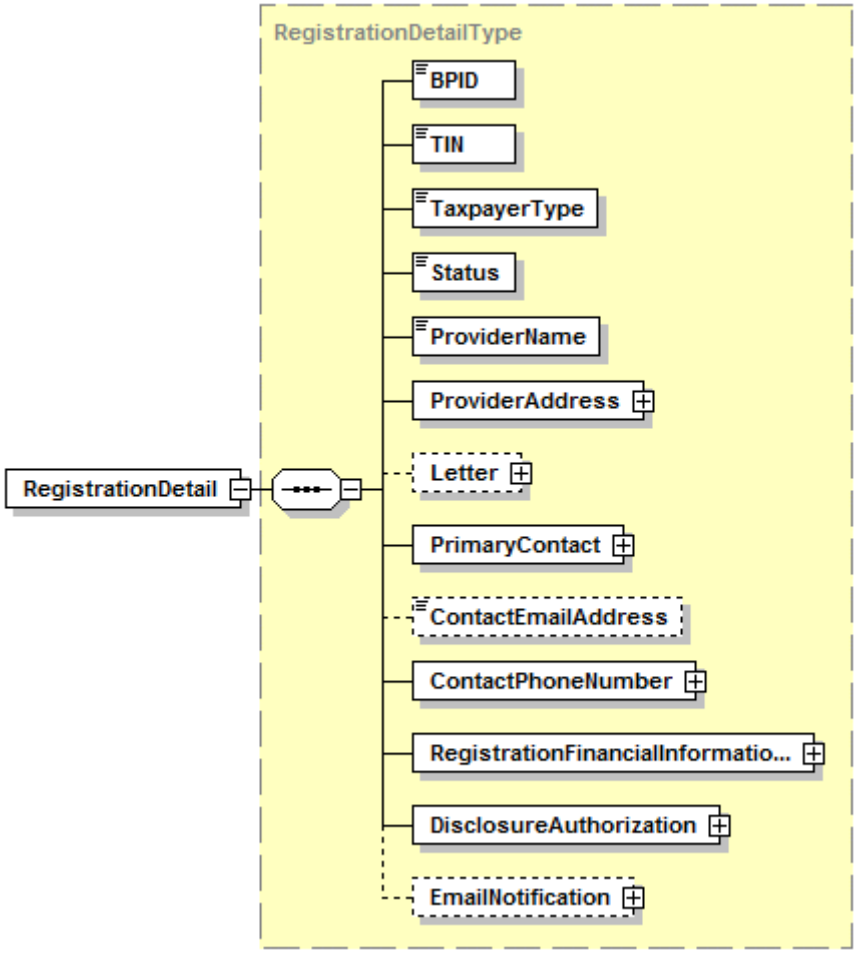

Figure 12 - Registration Detail

BATCH PROVIDER ACCOUNT MANAGEMENT

CHANGE MASTER PASSWORD

A batch provider may change their master password at any time. A batch provider may also receive a CPR (Change Password Required) status as a response from any request that requires authentication. When the CPR status is received, it indicates that the batch provider must change their password before proceeding. New passwords must not be the same as the previous five passwords. Change password is a synchronous request.

The XML schema element that represents a batch provider change password request is <BpChangeMasterPasswordRequest>. Responses are instances of the XML schema element <BpChangeMasterPasswordResponse>.

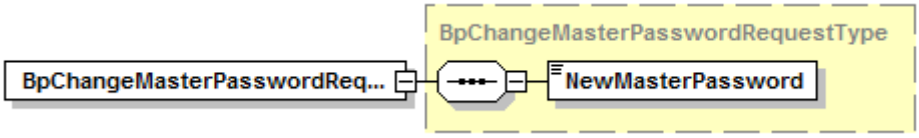

Figure 13 - Change Password Request

CHANGE MASTER PIN

A batch provider may change their Master PIN at any time. Change PIN is a synchronous request.

The XML schema element that represents a batch provider change PIN request is <BpChangeMasterPINRequest>. Responses are instances of the XML schema element <BpChangeMasterPINResponse>..

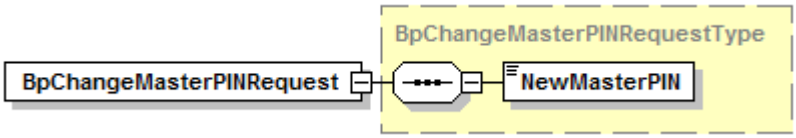

Figure 14 - Change PIN Requests

BATCH PROVIDER ENROLLMENT TRANSACTIONS

SUBMIT ENROLLMENT (NEW, EDIT, EDIT FI, TERMINATE)

The enrollment process associates a taxpayer with the Batch Provider. The XML schema element that represents a batch provider enrollment request is <BpEnrollmentRequest>. Responses are instances of the XML element <BpEnrollmentResponse>. Enrollment requests are processed by the IPS provider asynchronously.

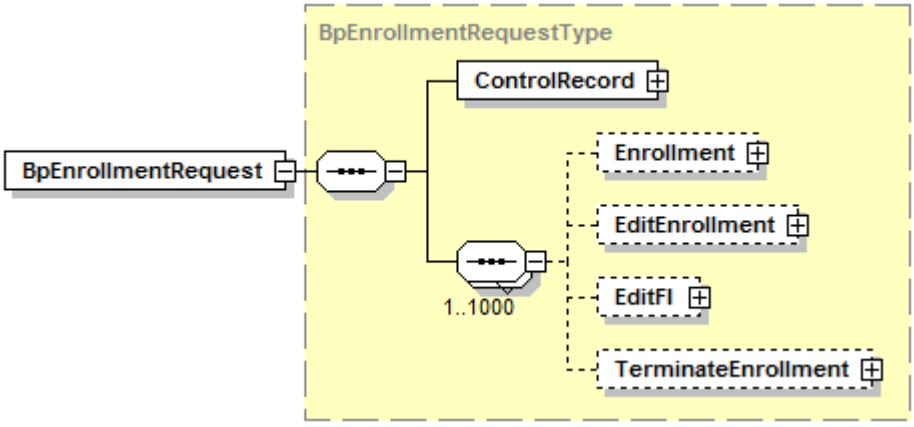

Figure 15 - Enrollment Request

Each request contains a Control Record, and up to 1000 Enrollments.

A Control Record is a unique combination of Date and Sequence Number for the transaction. The Enrollments sent in the batch will be linked to this Control Record such that they can be reconciled later on in enrollment synchronization.

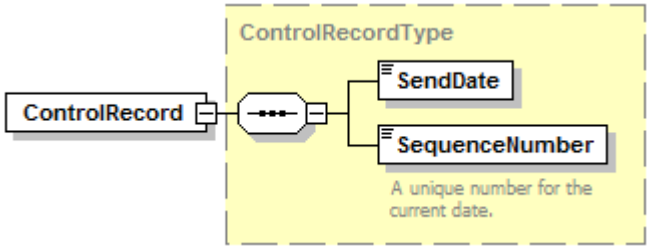

Figure 16 - Control Record

The <Enrollment> element is used for creating new Enrollments. It contains basic taxpayer information and the taxpayer's financial information is they are not using the Batch Provider's Master Account.

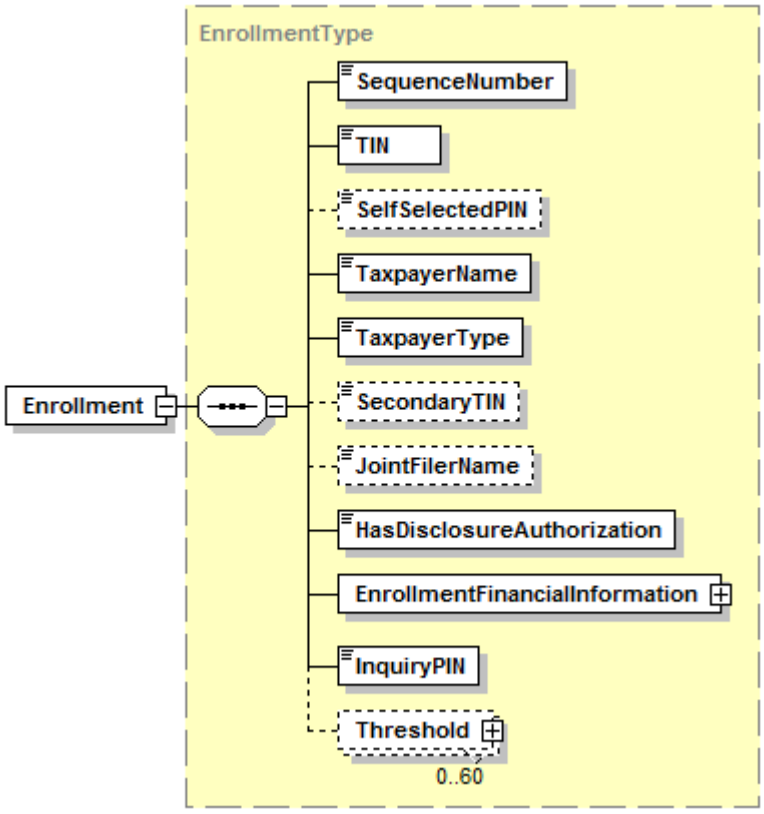

Figure 17 - Enrollment

The <EditEnrollment> element has a subset of the new Enrollment because some changes have implications that require a new Enrollment to be created.

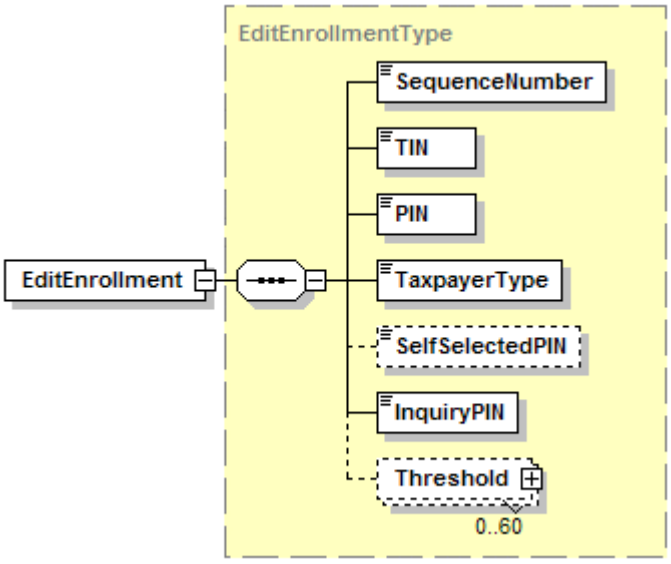

Figure 18 - EditEnrollment

The <EditFI> element is used for changing the bank account information for an enrolled taxpayer.

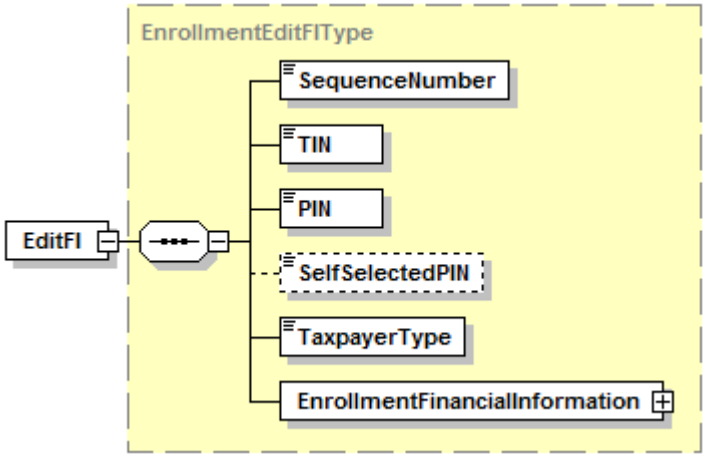

Figure 19 - Enrollment Edit FI

Finally, an Enrollment can be terminated using the <TerminateEnrollment> element.

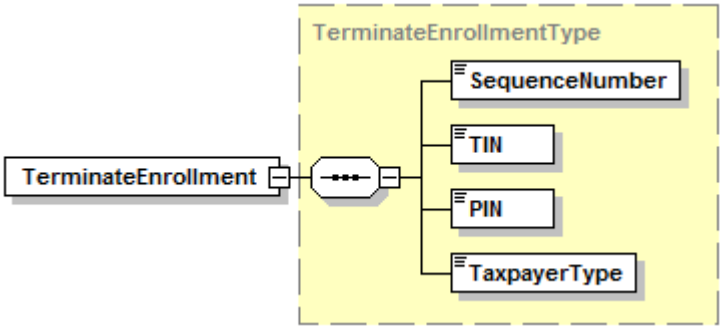

Figure 20 - Terminate Enrollment

ENROLLMENT SYNCHRONIZATION

Enrollment synchronization is used to synchronize client enrollments with server enrollments for a particular batch provider. The XML schema element that allows batch providers to synchronize enrollments is <BpEnrollmentSynchRequest>. Responses are instances of the XML schema <BpEnrollmentSynchResponse>. All enrollments for a batch provider that have had activity since the <FromActivityDate> to the current date are returned in the response for an enrollment synchronization. Enrollment synchronization is a synchronous request.

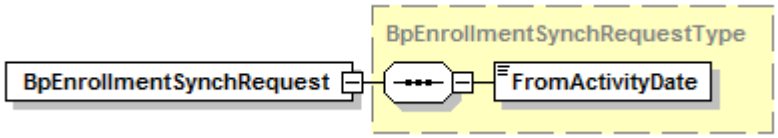

Figure 21 - Enrollment Synch Request

The response contains all the Enrollments from the activity date, with a detail record for each one:

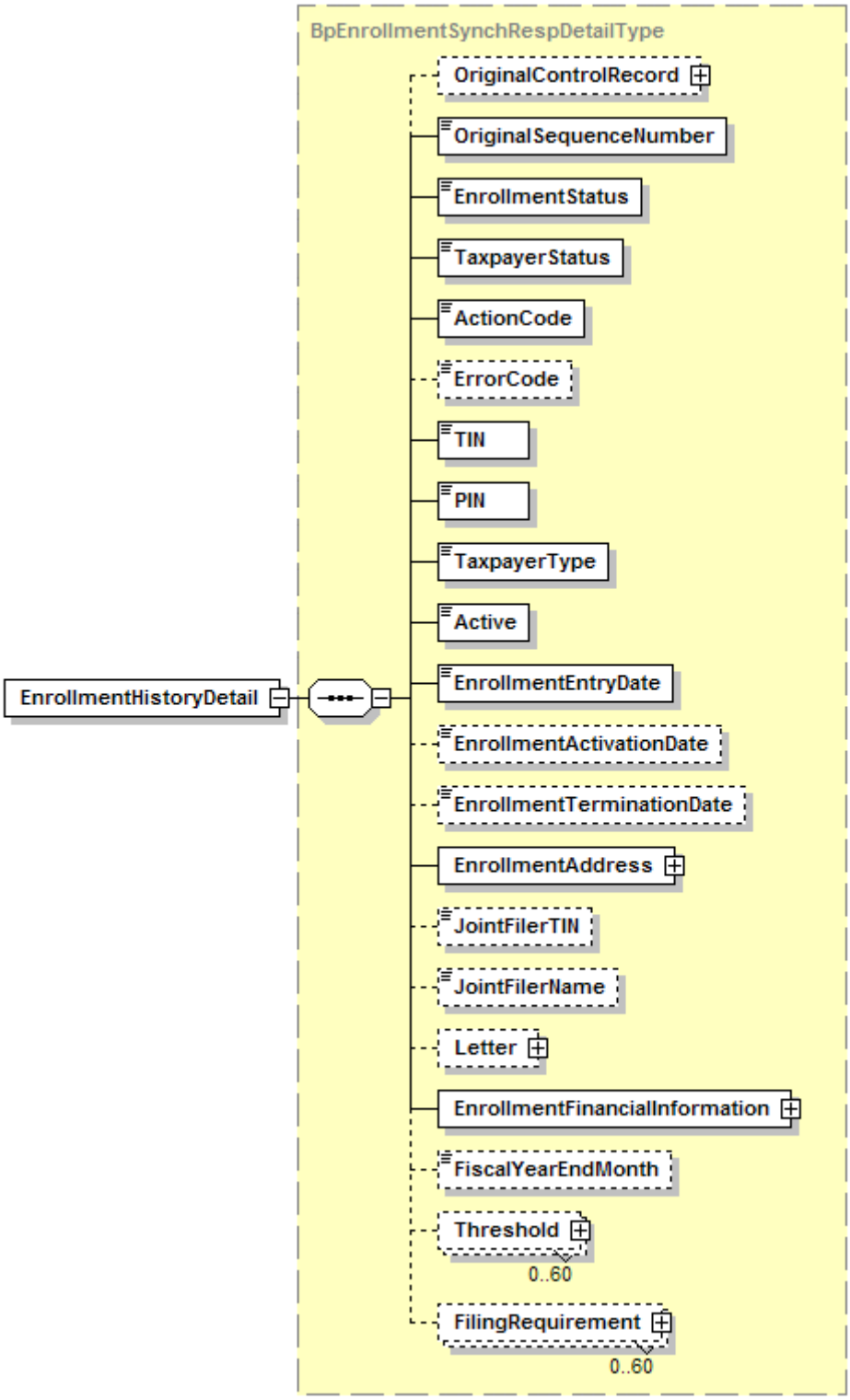

Figure 22 - Enrollment History Detail

BATCH PROVIDER PAYMENT TRANSACTIONS

SUBMIT BATCH PROVIDER PAYMENTS

The batch provider submit payments transaction allows batch providers to submit payments and payment cancellations to EFTPS for processing. The XML schema element for the Submit Batch Provider Payments request is <BpPaymentRequest>. Responses for the request are instances of the XML schema element <BpPaymentResponse>. A previously registered batch provider will need to obtain an master password from the EFTPS VRS for full authentication credentials. Batch provider authentication credentials must be sent as part of this request.

Batch provider payments are processed asynchronously by the EFTPS. A payment request is received by the IPS application and if the XML and authentication credentials are valid, the IPS application will immediately send back a response of OK. EFTPS may actually take several hours to complete the processing for these payments. After this time, the batch provider may send in a <BpPaymentSynchRequest> to receive a <BpPaymentSynchResponse> with detailed information about the payments that have been processed.

Two types of payments may be made through the IPS: bulk (single) debit or multiple debits. In a bulk debit, multiple tax payments will be aggregated and debited to the batch provider as a single ACH debit

There are four different payment types for a batch; payments, bulk payments, payment cancellations, and bulk payment cancellations. Bulk payments and bulk payment cancellations must be in a separate batch. A batch can contain up to 5000 tax payments or payment cancellations. Important facts about payment requests:

- All XML instance documents must conform to the XML schema element <BpPaymentRequest>.
- All settlement dates must be valid business days at least one day in the future. The cutoff time for a business day is 19:00 Eastern Time.
- Payments that have a settlement date less than two days in the future cannot be cancelled.
- Payments may only be made for taxpayers who are enrolled under the batch provider submitting the payment.
- Payments that fail business rule validation on the server will not cause an entire payment request to fail. The invalid payments will simply not be processed and will be returned in the response.
- Payments must be made for a valid tax period for the tax type code submitted.

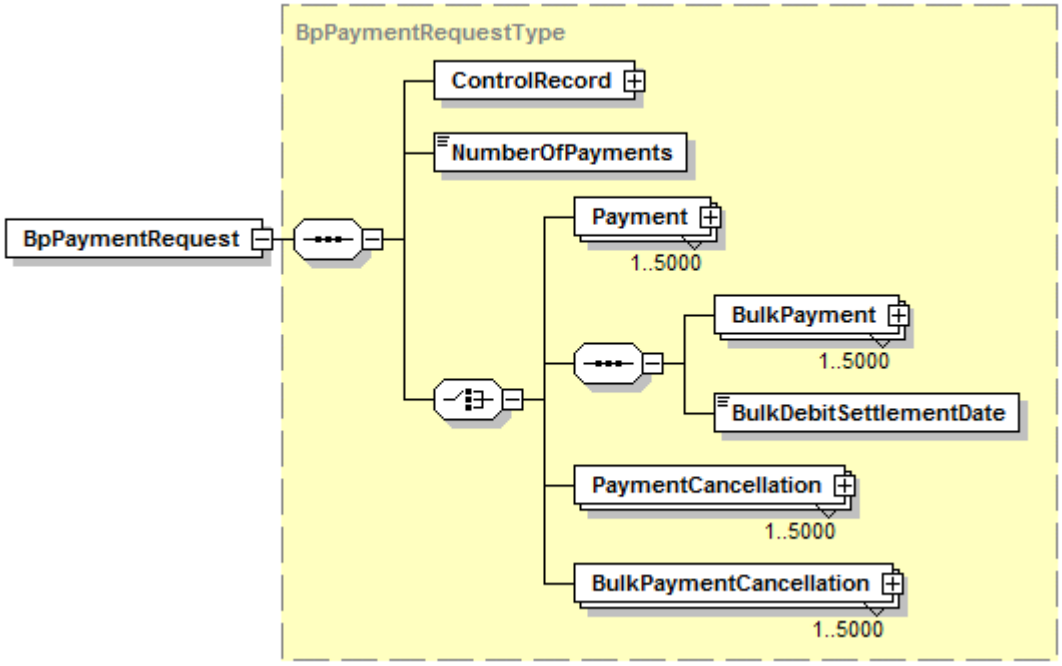

Figure 23 - BP Payment Request

The maximum number of payment elements in a request is 5000.

The <BpPaymentResponse> element can contain a transaction level error, or a set of PaymentResponseDetail elements with a status for each payment that was sent in the batch. If the <Status> is ERR, an <ErrorCode> will be supplied to provide more detail about the type of error.

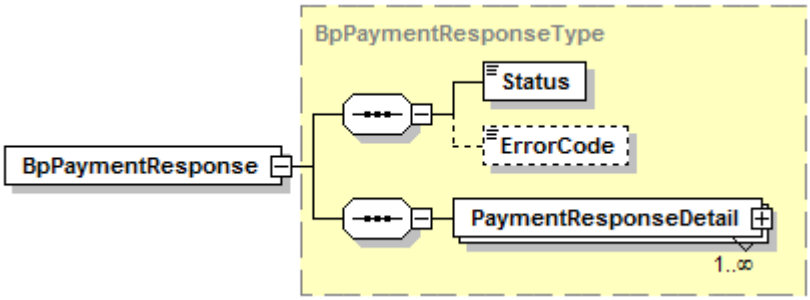

Figure 24 - BP Payment Response

- Multiple Payment Batch

This transaction uses the <Payment> element to submit a batch of payments for processing to EFTPS. The batch of payments has all the payment data specified including settlement date for each payment.

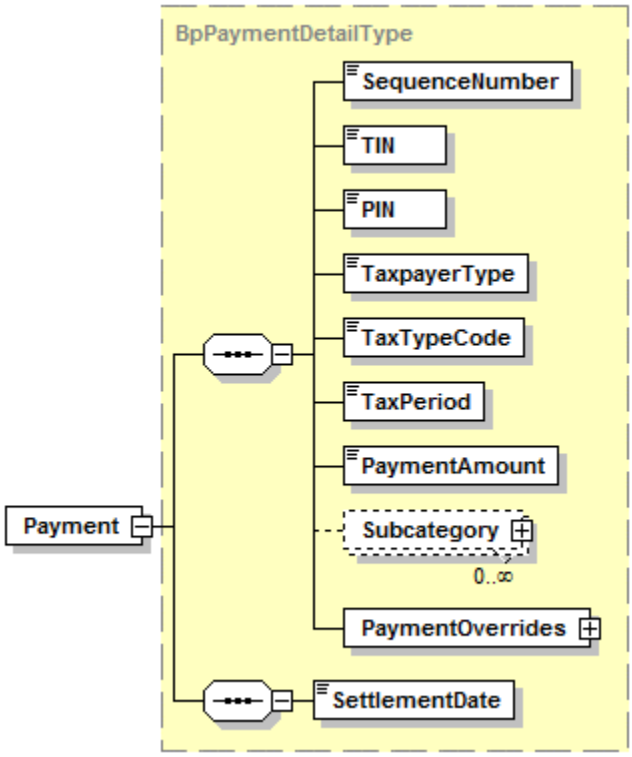

Figure 25 - Payment

For certain tax forms there is no tax period. In such cases, the tax period that should be submitted is "CCYY12".

From 0 – 99 subcategories are allowed in a payment. The number of subcategories is dependent on the tax form for which the payment is being made.

- Bulk Payment Batch

Bulk debit payments are made by using the <BulkPayment> element. Bulk debit payments may only be made for taxpayers who are enrolled to pay using the batch provider's master account. The batch provider must have a registered bank account in order to choose the bulk payment option at payment time. Bulk payments may not be initiated by batch providers who registered with the RegistrationFinancialInformation method of <UseTaxpayerAccount>. Batch providers may change their payment method by initiating a batch provider edit registration FI request.

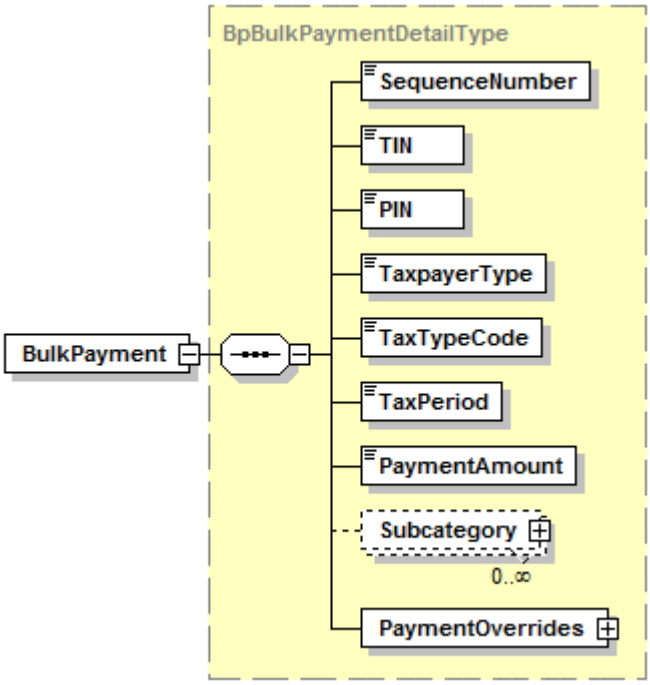

Figure 26 - Bulk Payment

Payment Cancellation Batch

Payment cancellations are initiated by using the <PaymentCanellation> element. This element includes the sequence number and the EFT number of the payment that should be cancelled.

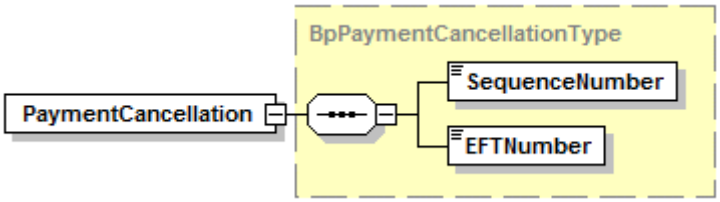

Figure 27 - Payment Cancellation

Bulk Payment Cancellation Batch

Due to the nature of bulk payments, bulk payment cancellation is a separate request. Bulk payments are cancelled by using the <BulkPaymentCancellation> element. This element contains the bulk payment EFT number of the bulk payment. Bulk payments may only be cancelled in their entirety. Should a batch provider wish to cancel only part of a bulk payment, the entire bulk payment must first be cancelled and then the remaining payments should be sent as a new bulk payment request. Bulk payments may not be cancelled if the settlement date of the bulk payment is less than two days in the future.

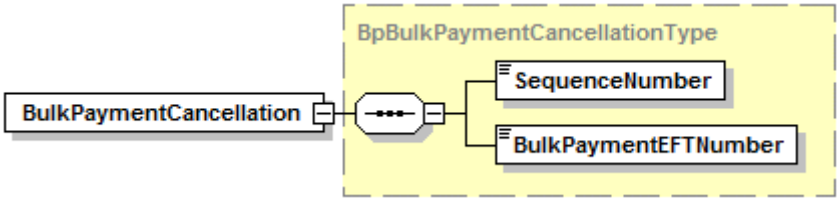

Figure 28 - Bulk Payment Cancellation

PAYMENT SYNCHRONIZATION

Payment synchronization allows a batch provider to retrieve their detailed payment history from a specified date. Payment synchronization returns all payments that have had activity from the date specified in the request.

The request must be an instance of XML schema element <BpPaymentSynchRequest>. The response is an instance of XML schema element BpPaymentSynchResponse>.

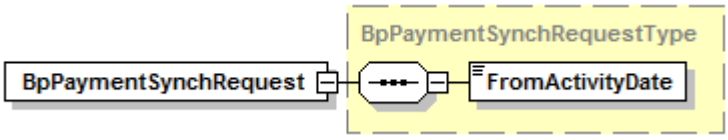

Figure 29 - Payment Synch Request

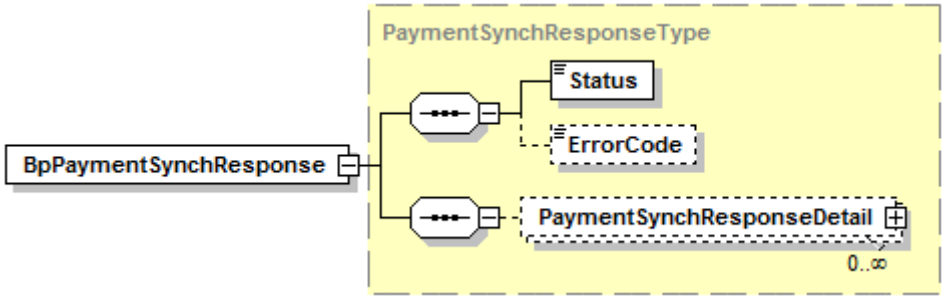

Figure 30 - Payment Synch Response

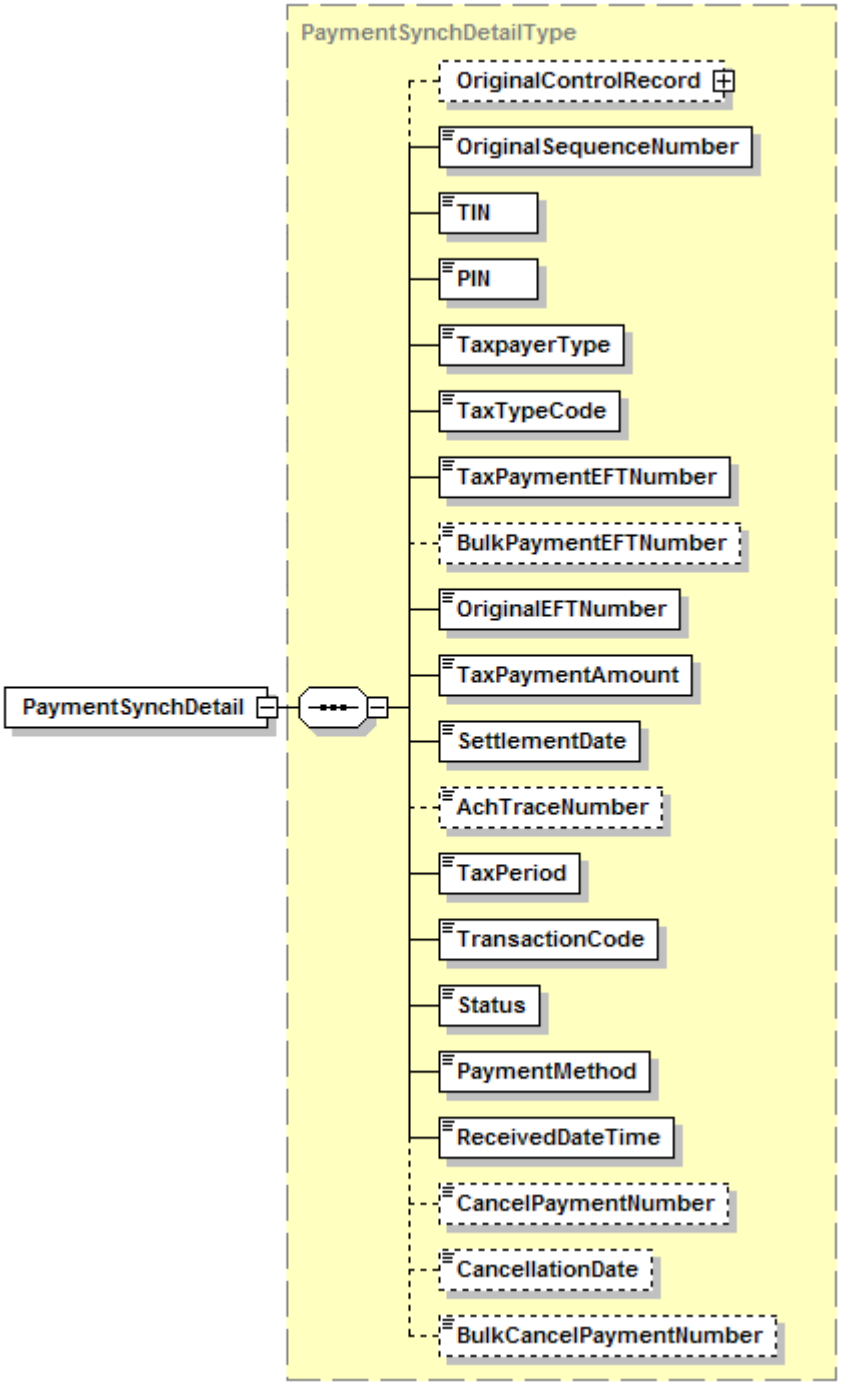

Figure 31 - Payment Synch Detail

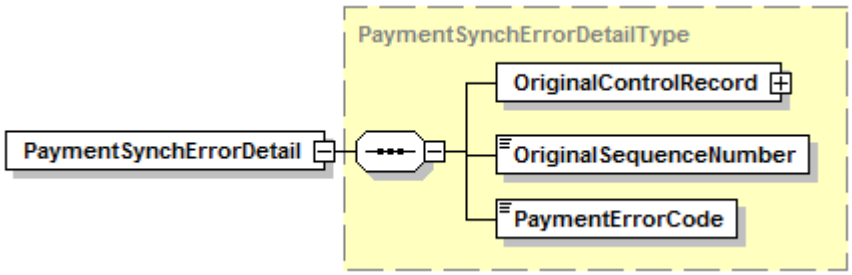

Figure 32 - Payment Synch Error Detail

Note that payments that were submitted as bulk debits have both a bulkPaymentTraceNumber and a taxPaymentEFTNumber. For these bulk payments, the bulkPaymentTraceNumber corresponds to the ACH debit whereas the taxPaymentEFTNumber is the EFT Number the taxpayer may use to refer to their payment. If a bulk payment was cancelled, the bulk payment cancellation trace number will also be returned for each tax payment in the response.

THIRD PARTY TRANSMITTER TAXPAYER TRANSACTIONS

The EFTPS IPS allows the following transactions for taxpayers: payments, payment cancellations, and payment history. Taxpayer payment requests are unlike batch provider payment requests in that only one payment or payment cancellation may be made per request. Taxpayer payments and payment cancellations are also transacted via separate URIs than the batch provider payment transactions.

All taxpayer payment requests are made by third-party software providers utilizing taxpayer authentication credentials. If authentication fails for a taxpayer, an AUTH status will be sent back in the response. If a taxpayer's password is expired, the IPS will send back a CPR status in the response. This status indicates that they should use EFTPS-OnLine web to create a new password and then retry their transaction once their password has been successfully changed.

SUBMIT TAXPAYER PAYMENTS AND PAYMENT CANCELLATIONS

The XML schema element that represents a taxpayer payment request is <TpPaymentRequest>. The XML schema element that represents the response is <TpPaymentResponse>.

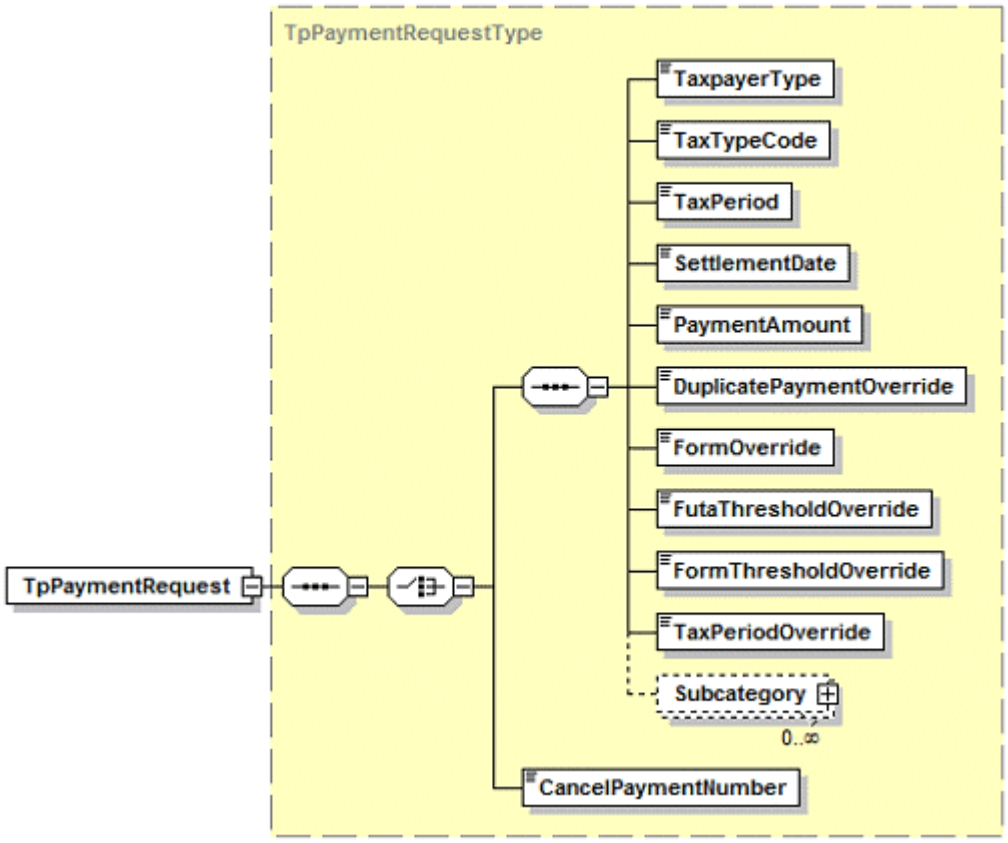

Figure 33 - Taxpayer Payment Request

The following information is for submitting a taxpayer payment request:

- This request is processed in real time.

- This request may be made only for those taxpayers who are enrolled with EFTPS. The taxpayer's authentication credentials must be valid and unexpired.
- A payment request that has a settlement date of less than 2 days in future cannot be cancelled.
- Only one payment or cancellation may be made in a taxpayer payment request.

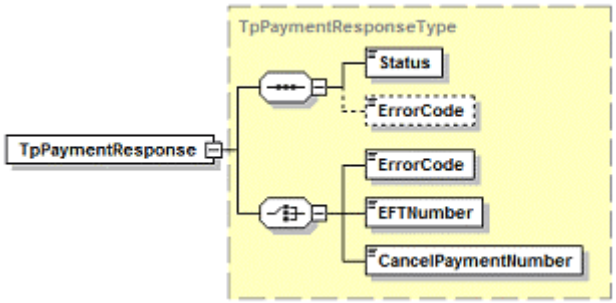

Figure 34 - Taxpayer Payment Response

TAXPAYER PAYMENT SYNCHRONIZATION

Taxpayer payment synchronization allows a taxpayer to retrieve their payment history either for a specified time period or for a given payment EFT number. Payment synchronization returns all payments that have had activity within the time period specified by the timestamps in the request.

The request must be an instance of XML schema element <TpPaymentSynchRequest>. The response is an instance of XML schema element <TpPaymentSynchResponse>.

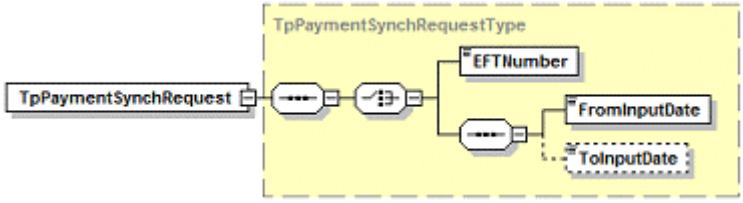

Figure 35 - Taxpayer Payment Synch Request

The following information is for submitting a taxpayer payment history request:

- This request is processed synchronously.
- This request may be made only for those taxpayers who are enrolled with EFTPS. The taxpayer's authentication credentials must be valid and unexpired.
- At most, the last 16 months of payment history for the taxpayer may be returned by this request.

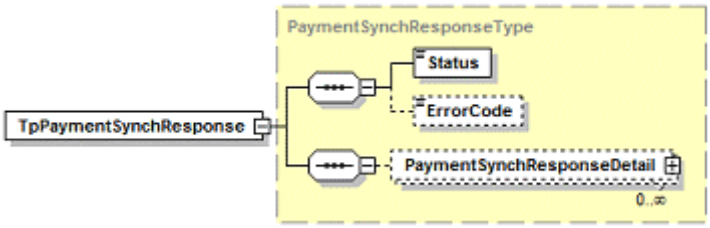

Figure 36 - Taxpayer Payment Synch Response

UTILITY FUNCTIONS

The IPS utility functions allow both batch providers and third party software developers to retrieve data that is custom to EFTPS and used within EFTPS IPS transactions. Requests for utility functions require the IPSHeader with the Batch Provider Authentication.

BATCH PROVIDER MESSAGE REQUEST

Message requests are used to look up any important messages the EFTPS may have for the batch provider. Message responses contain indicators that notify the batch provider whether any of the common utility data has been updated (country codes, holidays, and tax forms).

The XML schema element that represents a batch provider message request is <BpMessageRequest> Responses are instances of the XML schema element <BpMessageResponse>.

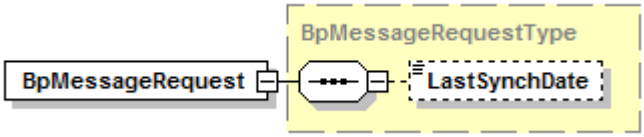

Figure 37 - Message Request

The LastSynchDate element is used to restrict the set of messages returned. If this element is not present, all messages will be returned.

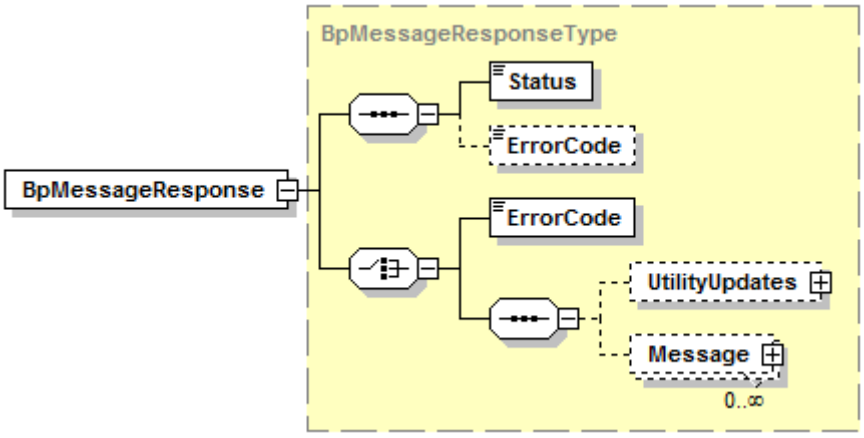

Figure 38 - Message Response

GET HOLIDAYS

The Get Holidays Utility returns a list of the banking holidays for the next 18 months. The XML schema element that represents a batch provider lookup request is <HolidayRequest>. Responses are instances of the XML schema <HolidayResponse>.

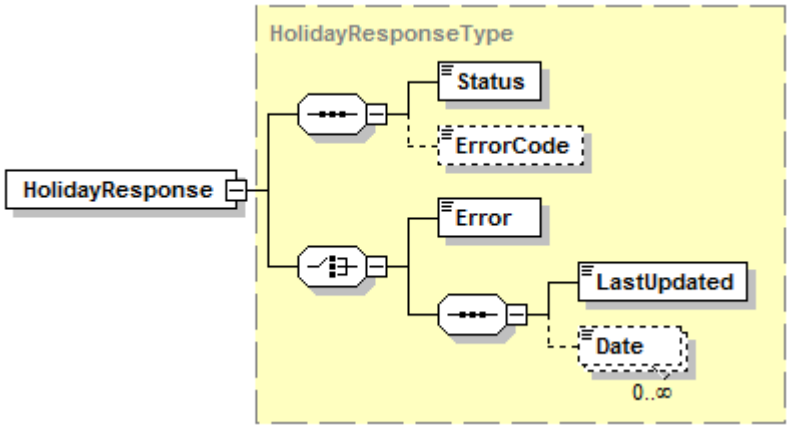

Figure 39 - Holiday Response

GET TAX FORMS

The Get Tax Forms Utility returns a list of the tax forms and related tax information. The XML schema element that represents a batch provider lookup request is <TaxFormRequest>. Responses are instances of the XML schema <TaxFormResponse>.

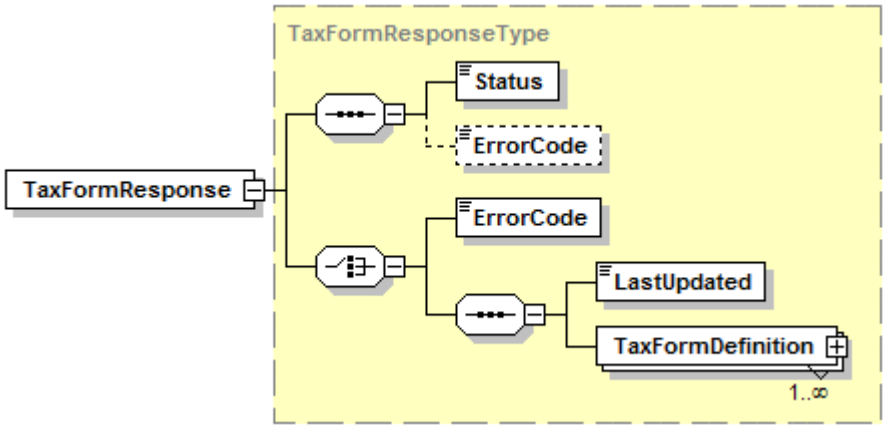

Figure 40 - Tax Form Response

GET COUNTRY CODES

The Get Country Code Utility returns a list of the countries recognized by EFTPS. The XML schema element that represents a batch provider lookup request is <CountryCodeRequest>. Responses are instances of the XML schema <CountryCodeResponse>.

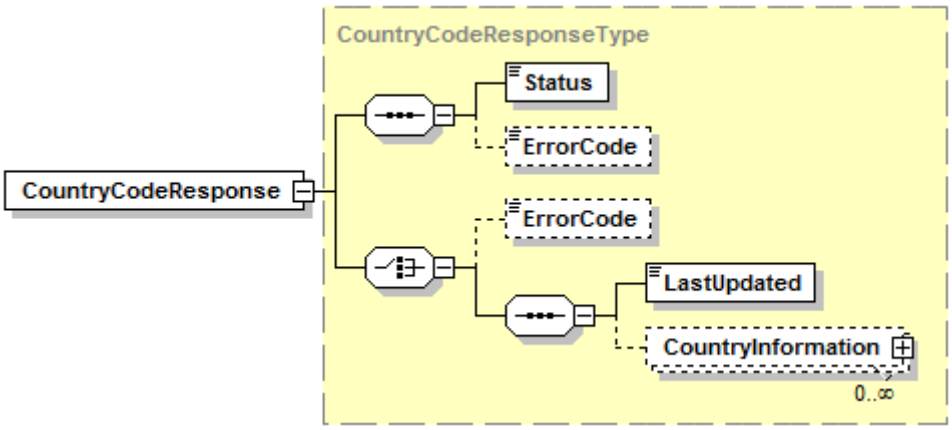

Figure 41 - Country Code Response

APPENDIX A: INVOCATION / TRANSPORT APPROACHES

Our approach was to develop an XML schema library that modernized batch provider file exchanges and facilitated taxpayer payments to EFTPS through a new channel. The schema defines transactions and unique XML elements for request and responses. Different invocation and transport approaches can be developed over time to satisfy new requirements and utilize other technologies. Each approach must address invocation and authentication for each of the identified transactions.

COMPRESSED XML / HTTPS MULTI-PART POST TRANSPORT

The initial implementation of an invocation approach utilizes XML over HTTP/HTTPS. HTTP request/response paradigm is utilized through the concept of URIs that represents specific EFTPS transactions. Each IPS transaction is invoked through a unique URI as shown in the table below. All IPS transactions will be independent, stateless, and synchronous consisting of a request and a response. The processing of the request may occur after the initial response is returned to achieve the asynchronous behavior. Because each transaction is stateless, each request that requires authentication must supply the authentication credentials in the request header.

The transport approach is based on HTTPS Multi-part Post over the Internet. The content type of the HTTPS Post must be "multipart/form-data" and the XML encoded request should be assigned the form-data name of "request". All requests and responses must be compressed utilizing the common GZIP compression algorithm. The IPS application runs on Eastern Time. All dates submitted to the IPS application are validated against Eastern Time.

The shared utility transactions do not require authentication and have no request data. They are accessed using an HTTPS GET instead of a POST. The xml responses for all utility functions are compressed using the GZIP compression algorithm.

Request Header / Authentication Approach

Authentication credentials must be provided as request header parameters within the HTTPS POST to every URI that requires authentication. The authentication requirements for each transaction are defined in Table 1. The data will be placed in the HTTP request header under "IPSHeader" with the value of the XML element of RequestHeader. Similarly, the ResponseHeader is returned in the response as a header under the value "IPSHeader".

Basic Steps in an HTTPS Multipart Transaction

1. A request in the form of an HTTPS POST with an XML payload is received at an EFTPS IPS URI.
2. The authentication credentials are pulled from the header and validated.
3. The XML is uncompressed and validated against the appropriate schema.
4. The XML payload is validated by the business rules pertaining to the request.
5. If the contents are valid, the appropriate EFTPS transactions are initiated.
6. A response is set back to the user via HTTPS.

Sample HTTPS POST

```
POST /batch_provider/registration/synch HTTP/1.1
IPSHeader: <RequestHeader><ProcessType>T</ProcessType>
              <SoftwareInfo>
                  <SoftwareID>123456789</SoftwareIDVendor>
                  <SoftwareVersion>1.0</SoftwareVersion>
              </SoftwareInfo>
               <BpAuthentication>
                   <BPID>000000000</BPID>
                   <PIN>0000</PIN>
                   <InternetPassword>000000</InternetPassword>
               </BpAuthentication>
           </RequestHeader>
Content-Type: multipart/form-data; boundary=”----SEP”
----SEP
Content-Disposition: form-data; name="request"; filename="request"
Content-Type: application/gzip; charset=UTF-8
Content-Transfer-Encoding: binary

<?xml version="1.0" encoding="UTF-8"?>
<BpRegistrationSynchRequest>
<!-- content eliminated for brevity -->
</BpRegistrationSynchRequest>
----SEP
```

Transaction Summary

Transaction	URI
Registration	
Submit New Registration	/batch_provider/registration/submit/new
Submit Taxpayer Registration	/batch_provider/registration/submit/tp
Change Registration	/batch_provider/registration/submit
Synchronize Registration	/batch_provider/registration/synch
Payment	
Submit Payments	/batch_provider/payment/submit
Get Payment Request Status	/batch_provider/payment/status
Synchronize Payment	/batch_provider/payment/synch
Enrollment	
Submit Enrollments	/batch_provider/enrollment/submit
Get Enrollment Request Status	/batch_provider/enrollment/status
Enrollment Synchronization	/batch_provider/enrollment/synch
Account Management	
Change Password	/batch_provider/account/change_password
Change Master Pin	/batch_provider/account/change_pin
Lookup Request	/batch_provider/account/lookup
Message Request	/batch_provider/account/message
Taxpayer Payment	
Submit Payments	/taxpayer/payment/submit
Payment Synchronization	/taxpayer/payment/synch
Utilities	
Get Holidays	/batch_provider/util/holidays
Get Tax Forms	/batch_provider/util/tax_forms
Get Country Codes	/batch_provider/util/countries
Get Error Codes	/batch_provider/util/errors